

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-105058

(43)Date of publication of application : 24.04.1998

(51)Int.Cl.

G09C 1/00

(21)Application number : 08-254057

(71)Applicant : HITACHI SOFTWARE ENG CO LTD

(22)Date of filing : 26.09.1996

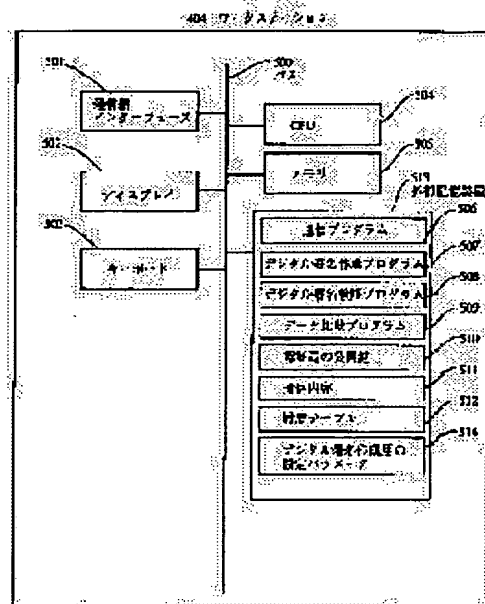
(72)Inventor : TSUTSUMI TOSHIYUKI

## (54) DATA GUARANTEE SYSTEM

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To secure the perfectness of data guaranteed by a transmitter even when these data are inspected by calculating a digital signature for newly guaranteeing the perfectness of communication contents by returning the communication contents deleted/changed by an inspector or an inspection process to the transmitter.

**SOLUTION:** The transmitter stores the copy of two pieces of received data in the history table of an external storage device 513. Next, the transmitter executes a digital signature preparation program 507 in an external storage device 513 of a work station 404 on a memory 505 of the work station 404 by applying the setting parameter for digital signature preparation of the work station 404 to be uniquely determined by a unidirectional function algorithm identifier contained in the received communication data to this program 507 and calculates the digital signature of the transmitter corresponding to the confirmed inspected communication contents. Afterwards, the transmitter prepares communication data in prescribed data structure from the confirmed inspected communication data and the selected digital signature and transmits these data.



## LEGAL STATUS

[Date of request for examination] 12.06.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3476171

[Date of registration] 26.09.2003

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-105058

(43) 公開日 平成10年(1998) 4月24日

(51) Int.Cl.<sup>5</sup>

G 0 9 C 1/00

識別記号

6 4 0

F I

G 0 9 C 1/00

6 4 0 Z

6 4 0 D

6 4 0 E

審査請求 未請求 請求項の数 1 O L (全 13 頁)

(21) 出願番号 特願平8-254057

(22) 出願日 平成8年(1996) 9月26日

(71) 出願人 000233055

日立ソフトウェアエンジニアリング株式会  
社

神奈川県横浜市中区尾上町6丁目81番地

(72) 発明者 堤 俊之

神奈川県横浜市中区尾上町6丁目81番地

日立ソフトウェアエンジニアリング株式会  
社内

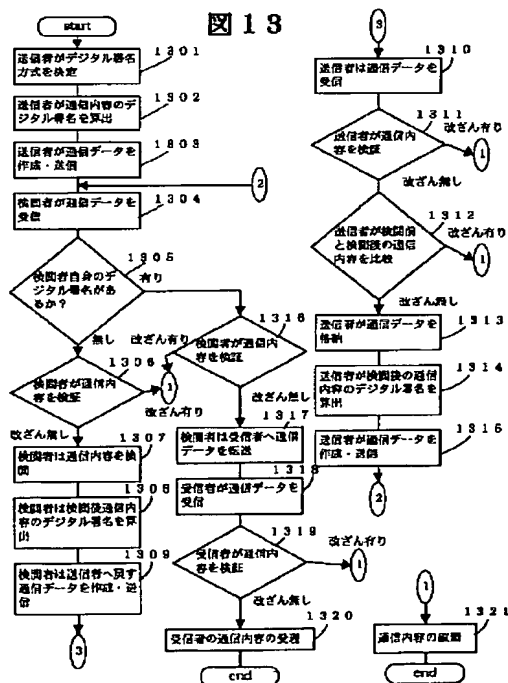
(74) 代理人 弁理士 秋田 収喜

(54) 【発明の名称】 データ保証システム

(57) 【要約】

【課題】 送信者と受信者の間で通信される通信内容が途中通信経路の端末で検閲され、削除されるシステムであって、検閲された通信内容であっても、受信者が送信者の保証したデータのデータの完全性を確認できる。

【解決手段】 検閲者もしくは、検閲プロセスが修正・変更した通信内容を送信者に戻して新たに通信内容の一貫性を保証するデジタル署名を計算する。



## 【特許請求の範囲】

【請求項 1】 通信網によって相互に接続された複数の端末からなり、複数の端末を中継してデータを通信する通信システムにおいて、

送信者と受信者の間で通信される通信データが途中通信経路の検閲端末で検閲処理が行われる環境にある場合、前記検閲端末が行う検閲処理により送信者の送信した通信データを検閲し、検閲された通信データと検閲前の通信データを前記検閲端末のデジタル署名とともに送信元に返送するステップと、

検閲を受けた通信データの返送を受けた送信者のデジタル署名プロセスが、検閲前の通信データと検閲された通信データとを比較し、検閲された通信内容に対してデジタル署名を行い、検閲端末を介して、受信者に転送するステップとからなり、

検閲端末から受信した通信データの受信者が、受信した通信内データとデジタル署名からデータの一貫性が確認できることを特徴とするデータ保証システム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、ネットワークを介してデータの交換を行うデータ転送システムに関わり、特に、転送されたデータの完全性を保証するデータ転送システムに関するものである。ここで、データの完全性とは、送信者の送信したデータと受信者の受信したデータが完全に一致することをいう。

## 【0002】

【従来の技術】ネットワークを介し、データの交換を行うデータ転送システムにおいて、転送されているデータの全部もしくは一部が、途中経路で変更・削除されることは、安全上の重大な問題となる。そこで、現在は一方方向性関数と公開鍵暗号から作られるデジタル署名を利用することによって、安全性を確保し、盗聴、秘密の漏洩などの問題が、発生しないようにしている。

【0003】この技術について、図 1、図 2 および図 3 を用いて説明する。

【0004】具体的に、図 1 に示すように送信者 101 と受信者 102 が一方方向性関数アルゴリズム 103 と公開鍵暗号アルゴリズム 104 と送信者の公開鍵 105 を共有しており、送信者 101 は自分の個人鍵 107 を保持している状態で、送信者 101 の持っている通信内容 106 を受信者 102 に通信する場合を図 2 の流れ図に従って説明する。

【0005】ここで、一方方向性関数とは、任意の長さの入力データに対して、固定長の出力データを算出し、同じ入力データに対しては同じ出力データを算出し、出力データから入力データを推測することが非常に困難であるような特徴を持った関数である。

【0006】また、個人鍵とは、公開鍵暗号で任意の受信者に割り当てられる 2 つの鍵のうちの 1 つを示してい

る。

【0007】公開鍵暗号とは、暗号化と復号で異なる鍵を利用する暗号方式であり、情報の受信者に、公開鍵と呼ばれる鍵と対応する個人鍵と呼ばれる鍵をペアで割り当てて、公開鍵を公に公開し、個人鍵を秘密に保持している状態で、情報を送りたい送信者が、受信者の公開鍵でその情報を暗号化することで、安全に受信者に送ることができる仕組みを提供するものである。

【0008】この技術は、公開鍵で暗号化した情報は、対応する個人鍵でしか復号できない性質を利用して実現されているからである。さらに、公開鍵暗号は、個人鍵で暗号化した情報も、対応する公開鍵でしか復号できないので、送信者が自分の個人鍵で情報を暗号化して、それを受信者が送信者の公開鍵で復号すれば、送信者の認証としても利用することができる。

【0009】図 2 において、まず、送信者 101 は送信する通信内容 106 を入力として一方方向性関数アルゴリズム 103 の出力であるハッシュ値を算出する（ステップ 201）。次に送信者 101 は、ステップ 201 で算出したハッシュ値を送信者 101 の個人鍵 107 と公開鍵暗号アルゴリズム 104 で暗号化する。これをデジタル署名と呼ぶ（ステップ 202）。デジタル署名の例を図 3 に示す。

【0010】次に、送信者 101 は通信内容 106 とステップ 202 で作成したデジタル署名を受信者 102 に送信する（ステップ 203）。

【0011】次に、受信者 102 はステップ 203 で送信された通信内容 106 とデジタル署名を受信する（ステップ 204）。

【0012】次に、受信者 102 はステップ 204 で受信した通信内容 106 を入力として一方方向性関数アルゴリズム 103 の出力であるハッシュ値を算出する（ステップ 205）。

【0013】次に、ステップ 204 で受信したデジタル署名を送信者 101 の公開鍵暗号アルゴリズム 104 と公開鍵 105 で復号する（ステップ 206）。次に、受信者 102 は、ステップ 205 で算出したハッシュ値とステップ 206 で復号したデジタル署名を比較する。同一データであれば、ステップ 208 へ進み、異なったデータであれば、ステップ 210 へ進む（ステップ 207）。送信者 102 は通信内容が改ざんされていなかったと判断する（ステップ 208）。

【0014】送信者 102 は通信内容が改ざんされていると判断する（ステップ 210）。

【0015】なお、ステップ 202 で開示されるデジタル署名については例えば、図 8 に示す通信内容に対して、一方方向性関数アルゴリズムとして R F C 1321 で規定されている M D 5 を利用し、公開鍵暗号アルゴリズムとして R S A 暗号を利用した場合のデジタル署名を図 3 に示す。

【0016】こうした方法は、インターネットの標準プロトコルとしてRFC1421～RFC1424に記述されている暗号電子メールシステムPEM (Privacy Enhanced Mail) やPhilip R. Zimmermannにより開発されたPGP (Pretty Good Privacy) の中に取り入れられている。

【0017】

【発明が解決しようとする課題】ところで、最近、インターネットの普及により、コンピュータネットワーク上で、青少年に害をなす猥褻な画像などの有害情報が閲覧可能になってしまっている。そこで政府やネットワークプロバイダが市民やユーザに有害な情報を提供しないように、通信内容の検閲を行っている。

【0018】この技術は、通信内容を提供するマシンへのアクセス権や通信内容全体の閲覧権を設定する方法で行われている。

【0019】しかし、従来の技術では、検閲者もしくは、検閲プロセスが受信者に暴力的イメージや性的表現などの有害な情報を与えないために、通信経路の途中で通信内容を検閲して、通信内容の一部を削除した場合に、通信内容の最終的な受信者は、チェックデータを計算できず、送信者の保証したデータの完全性を確かめることができない。

【0020】本発明の目的は、故意、悪意により通信内容の一部が削除されるような検閲を受けた場合でも、送信者の保証したデータの完全性を確保できるシステムを提案することにある。

【0021】

【課題を解決するための手段】この課題を解決するために、本システムでは、検閲者もしくは、検閲プロセスが削除・変更した通信内容を送信者に戻して新たに通信内容の完全性を保証するデジタル署名を計算することを提案している。この時、送信者が常に返送される変更・修正された通信内容を監視する必要は無く、自動的にデジタル署名を行い、受信者に再送信される。

【0022】

【発明の実施の形態】以下、本発明の実施形態の例を図面を用いて詳細に説明する。なお、同一番号は同様の部品・要素を表す。

【0023】図4において、401、402、403はそれぞれ送信者、検閲者、受信者であり、404、405、406は送信者、検閲者、受信者、認証者のワークステーションである。

【0024】ワークステーション404とワークステーション405は通信網407を介して相互に通信を行うことができ、ワークステーション405とワークステーション406は通信網408を介して相互に通信を行うことができる。そして、ワークステーション405とワークステーション407は、通信網407とワークステ

ーション405と通信網408を介して通信を行うことができる。送信者401や受信者402、検閲者403は、ユーザ、あるいは、プログラムを示している。

【0025】図5に示す送信者401のワークステーション404は、通信網との間でデータのやりとりを行う通信網インターフェース501と、ユーザにメッセージ等を表示するディスプレイ502と、ユーザがデータ等を入力するためのキーボード503と、演算処理を行うCPU504とメモリ505、通信プログラム506やデジタル署名作成プログラム507やデジタル署名検証プログラム508やデータ比較プログラム509や認証局の公開鍵510や通信内容511や履歴テーブル512やデジタル署名作成用の設定パラメータテーブル514が記録されている外部記憶装置513とを有しており、それらはバス500によって相互に接続されている。

【0026】ここで、認証局は任意の公開鍵の正当な所有者を承認して、その公開鍵にデジタル署名を発行する機関であることを示す。

【0027】図6は、設定パラメータテーブル516の構造を示したものである。600には利用可能な方向性関数アルゴリズム識別子がつけられている。601には利用可能な公開鍵暗号アルゴリズム識別子がつけられている。602にはそのアルゴリズムに対応した送信者401の個人鍵がつけられている。603には対応した送信者401の公開鍵がつけられている。1004は603の公開鍵について認証局が発行したデジタル署名が格納されている。

【0028】図7は、履歴テーブル512の構造を示したものである。701は検閲前の通信内容、702は通信内容701のデジタル署名、703は方向性関数アルゴリズム識別子、704は公開鍵暗号アルゴリズム識別子、705には検閲された通信内容、706は通信内容705のデジタル署名、707はデジタル署名706を施した署名者の名前、708には通信内容705を復号するための公開鍵が格納されている。

【0029】外部記憶装置513に記憶されている通信プログラム506は、他の端末との間でデータのやりとりを行う場合にその制御を行うプログラムである。

【0030】デジタル署名作成プログラム507は、プログラムに与えられた通信内容が改ざんされていないことを保証し、送信者を正しく識別できるデジタル署名を作成するプログラムである。

【0031】図9は、ワークステーション404～6間で通信するデータの構造を示している。901はデータ構造全体を表し、通信データと呼ぶ。通信データ901は本来、通信相手に伝えたい内容を示す通信内容902と主署名者パラメータ部912と副署名者パラメータ部913に分けることができる。

【0032】主署名者パラメータ部912は、メインの

10

20

30

40

50

デジタル署名者による通信内容の完全性を検証するためにデジタル署名903とデジタル署名を施した署名者名904、署名者の公開鍵905と署名者の公開鍵905に対する認証局のデジタル署名906、採用した一方向性関数アルゴリズム識別子909と公開鍵暗号アルゴリズム識別子910で構成されている。

【0033】副署名者パラメータ部913は、メインとは別のデジタル署名者による通信内容に対するデジタル署名907や署名を施したデジタル署名者名908を追加することができる。また、通信データ901は副署名者パラメータ部913を複数持つことができる。

【0034】デジタル署名検証プログラム508は、プログラムに与えられた通信データの通信内容とデジタル署名を比較して、通信内容の改ざんや送信者の正しい識別ができたことを確認するプログラムである。

【0035】データ比較プログラム509は、プログラムに与えられた検閲前の通信内容と検閲後の通信内容を比較して、検閲後の通信内容が検閲前の通信内容を削除して作られたものであることを確認するプログラムである。

【0036】図10に示す検閲者402のワークステーション405は、通信網との間でデータのやりとりを行う通信網インターフェース501と、ユーザにメッセージ等を表示するディスプレイ502と、ユーザがデータ等を入力するためのキーボード503と、演算処理を行うCPU504とメモリ505、通信プログラム506やデジタル署名作成プログラム507やデジタル署名検証プログラム508や検閲プログラム1101や認証局の公開鍵510やデジタル署名作成用の設定パラメータテーブル514や検閲する言葉の格納してある検閲ワードテーブル1102が記録されている外部記憶装置513とを有しており、それらはバス500によって相互に接続されている。

【0037】図11は検閲ワードテーブル1102の例を示す図である。検閲ワードテーブル1102は検閲者のポリシーが反映されており、例えば、外部に開示したくない組織内のサブ組織名や製品のコードネームや露骨でひわいな表現や相手を侮辱する表現などが格納されている。

【0038】検閲プログラム1101は、プログラムに与えられた通信内容に検閲ワードテーブルに格納されている表現があるか検索して、もしあった場合に、通信内容からその表現を削除するプログラムである。

【0039】図12に示す受信者403のワークステーション406は、通信網との間でデータのやりとりを行う通信網インターフェース501と、ユーザにメッセージ等を表示するディスプレイ502と、ユーザがデータ等を入力するためのキーボード503と、演算処理を行うCPU504とメモリ505、通信プログラム506やデジタル署名作成プログラム507やデジタル署名検

証プログラム508や認証局の公開鍵510やデジタル署名作成用の設定パラメータテーブル514が記録されている外部記憶装置513とを有しており、それらはバス500によって相互に接続されている。

【0040】図13を用いて、通信データが送信者で作成されてから受信者に受理されるまでの手順を説明する。

【0041】まず、送信者401は通信内容511のデータの完全性を保証するデジタル署名方式をワークステーション404の外部記憶装置513にあるデジタル署名作成用の設定パラメータテーブル514から選択する(ステップ1301)。

【0042】次に、送信者401はワークステーション404の外部記憶装置513にあるデジタル署名作成プログラム507に通信内容511とステップ1401で選択したデジタル署名作成用の設定パラメータを与えて、ワークステーション404のメモリ505上で実行させ、通信内容511に対する送信者401のデジタル署名を算出する(ステップ1302)。図8に通信内容の例を示し、図3にその通信内容に対するデジタル署名を示す。

【0043】次に、送信者401は通信内容511とステップ1301で選択された設定パラメータとステップ1302で算出されたデジタル署名から、図9に示したデータ構造の通信データを作成して、送信する(ステップ1303)。

【0044】次に、検閲者402がステップ1303で送信者401により作成・送信された通信データを受信する(ステップ1304)。

【0045】次に、検閲者402はステップ1304で受信した通信データの複数あるデジタル署名者名に検閲者402自身の名前がないかどうか確認する。あった場合はステップ1316へ進む。なかった場合は、ステップ1306へ進む(ステップ1305)。

【0046】次に、検閲者402はワークステーション405の外部記憶装置513にあるデジタル署名検証プログラム508に、ステップ1304で受信した通信データを与えて、ワークステーション405のメモリ505上で実行させ、通信データ内の通信内容が改ざんされていないか確認する。改ざんされていればステップ1321へ進む。改ざんされていなければステップ1307へ進む(ステップ1306)。

【0047】次に、検閲者402はワークステーション405の外部記憶装置513にある検閲プログラム1101に、ステップ1306で改ざんされていないこと確認された通信内容を与えて、ワークステーション405のメモリ505上で実行させて、検閲後の通信内容を得る。ここで、通信内容の検閲は、検閲プログラム1101で行わないで、人間である検閲者が手動で行う場合も想定している(ステップ1307)。

【0048】次に、検閲者402はワークステーション405の外部記憶装置513にあるデジタル署名作成プログラム507にステップ1304で受信した通信データ内に含まれる一方向性関数アルゴリズム識別子と公開鍵暗号アルゴリズム識別子で一意に決定できるワークステーション405のデジタル署名作成用の設定パラメータテーブル514上の設定パラメータを与えて、ワークステーション405のメモリ505上で実行させ、ステップ1307で検閲した通信内容に対する検閲者402のデジタル署名を算出する(ステップ1308)。

【0049】次に、検閲者402はステップ1307で検閲した通信内容とステップ1308で選択された設定パラメータとステップ1308で算出されたデジタル署名から、図9に示したデータ構造の通信データを作成し、さらに、ステップ1304で受信した通信データを連結して、送信者401に送信する(ステップ1309)。

【0050】次に、送信者401はステップ1309で検閲者402により作成・送信された連結された2つの通信データを受信する(ステップ1310)。

【0051】次に、送信者401はワークステーション404の外部記憶装置513にあるデジタル署名検証プログラム508に、ステップ1310で受信した2つの通信データをそれぞれ個別に与えて、ワークステーション404のメモリ505上で実行させ、通信データ内の通信内容が改ざんされていないか確認する。どちら一方の通信内容が改ざんされていなければステップ1321へ進む。どちらも改ざんされていなければステップ1312へ進む(ステップ1311)。

【0052】次に、送信者401はワークステーション404の外部記憶装置513にあるデータ比較プログラム509に、ステップ1311で検証した検閲前の通信内容と検閲後の通信内容を与えて、ワークステーション404のメモリ505上で実行させ、検閲後の通信内容が検閲前の通信内容を削除しただけのものであることを確認する。検閲後の通信内容が削除しただけのものであればステップ1313へ進む。それ以外はステップ1321へ進む(ステップ1312)。

【0053】次に、送信者401はステップ1310で受信した2つの通信データのコピーをを外部記憶装置513の履歴テーブルに格納する(ステップ1313)。

【0054】次に、送信者401はワークステーション404の外部記憶装置513にあるデジタル署名作成プログラム507にステップ1310で受信した通信データ内に含まれる一方向性関数アルゴリズム識別子と公開鍵暗号アルゴリズム識別子で一意に決定できるワークステーション404のデジタル署名作成用の設定パラメータテーブル514上の設定パラメータを与えて、ワークステーション404のメモリ505上で実行させ、ステップ1312で確認した検閲後の通信内容に対する送信

者401のデジタル署名を算出する(ステップ1314)。

【0055】次に、送信者401はステップ1312で確認した検閲後の通信内容とステップ1314で選択された設定パラメータとステップ1314で算出されたデジタル署名から、図9に示したデータ構造の通信データを作成して、送信する(ステップ1315)。こうして、ステップ1304に戻る。

【0056】次に、ステップ1305で検閲者402のデジタル署名があった場合の処理を以下に示す。

【0057】検閲者402はワークステーション405の外部記憶装置513にあるデジタル署名検証プログラム508に、ステップ1304で受信した通信データを与えて、ワークステーション405のメモリ505上で実行させ、通信データ内の通信内容が改ざんされていないか確認する。改ざんされていなければステップ1321へ進む。改ざんされていなければステップ1317へ進む(ステップ1316)。

【0058】次に、検閲者402はステップ1316で改ざんされていないことを確認された通信データを受信者403に向けて転送する(ステップ1317)。

【0059】次に、受信者403がステップ1317で検閲者402により転送された通信データを受信する(ステップ1318)。

【0060】次に、受信者403はワークステーション406の外部記憶装置513にあるデジタル署名検証プログラム508に、ステップ1318で受信した通信データを与えて、ワークステーション406のメモリ505上で実行させ、通信データ内の通信内容が改ざんされていないか確認する。改ざんされていなければステップ1321へ進む。改ざんされていなければステップ1320へ進む(ステップ1319)。

【0061】次に、受信者403は、ステップ1319でデータの完全性が確認された通信内容を受理する(ステップ1320)。

【0062】最後に、ステップ1306、1311、1312、1316、1319で通信内容に改ざんがあった場合の処理を示す。

【0063】改ざんがあった場合、送信者401、検閲者402、受信者403、いずれの場合も通信データを全て消去する(ステップ1321)。

【0064】デジタル署名作成プログラム507の動作手順を図14の流れ図で説明する。

【0065】与えられた通信内容を入力として、与えられたデジタル署名用の設定パラメータで指定された一方向性関数アルゴリズムでハッシュ値を算出する(ステップ1401)。

【0066】与えられたデジタル署名用の設定パラメータで指定された公開鍵暗号アルゴリズムと対応する個人鍵で、ステップ1401算出したハッシュ値を暗号化し

て、デジタル署名を算出する(ステップ1402)。

【0067】デジタル署名検証プログラム508の動作手順を図15の流れ図で説明する。

【0068】与えられた通信データの主署名者パラメータ部にある署名者の公開鍵のデジタル署名を取り出し、主署名者パラメータ部の公開鍵暗号アルゴリズム識別子で指定される公開鍵暗号アルゴリズムと外部記憶装置に513にある認証局の公開鍵510で復号する(ステップ1501)。与えられた通信データの主署名者パラメータ部にある署名者の公開鍵を入力として、主署名者パラメータ部の一方方向性関数アルゴリズム識別子で指定される一方方向性関数アルゴリズムでハッシュ値を算出する(ステップ1502)。

【0069】ステップ1501で復号したデジタル署名とステップ1502で算出したハッシュ値を比較する。同じデータであれば、ステップ1504へ進む。異なったデータであればステップ1510へ進む(ステップ1503)。

【0070】与えられた通信データの主署名者パラメータ部にある通信内容のデジタル署名を通信データの主署名者パラメータ部にある公開鍵暗号アルゴリズム識別子で指定される公開鍵暗号アルゴリズムと通信データの主署名者パラメータ部にある公開鍵で復号する(ステップ1504)。与えられた通信データの通信内容を入力として、主署名者パラメータ部の一方方向性関数アルゴリズム識別子で指定される一方方向性関数アルゴリズムでハッシュ値を算出する(ステップ1505)。

【0071】ステップ1504で復号したデジタル署名とステップ1505で算出したハッシュ値を比較する。同じデータであれば、ステップ1507へ進む。異なったデータであればステップ1510へ進む(ステップ1506)。通信データの通信内容が改ざんされていなかったと判断する(ステップ1507)。通信データの通信内容が改ざんされていると判断する(ステップ1510)。

【0072】データ比較プログラム508の動作手順を図16の流れ図で説明する。

【0073】最初に変数Iに「1」をセットする(ステップ1601)。与えられた検閲前の通信内容の先頭からI番目の文字データを取り出す(ステップ1602)。

【0074】同様に、与えられた検閲後の通信内容の先頭からI番目の文字データを取り出す(ステップ1603)。次に、ステップ1602とステップ1603で文字が取り出せたか確認する。ステップ1602とステップ1603の両方で文字データが取り出せれば、ステップ1605へ進む。逆に、ステップ1602とステップ1603の両方で文字データが取り出せなければ、ステップ1610へ。それ以外は、ステップ1611へ進む(ステップ1604)。

【0075】ステップ1603で得られた文字が、検閲文字であるならステップ1607へ。そうでなければ、ステップ1606へ進む。ここで、検索文字とは「■」を表す(ステップ1605)。

【0076】次に、ステップ1602で得られた文字とステップ1603で得られた文字を比較する。同じ文字データでならば、ステップ1607へ進む。異なった文字データであればステップ1611へ進む(ステップ1606)。

【0077】次に、変数Iの値を「1」増やし、ステップ1602に戻る(ステップ1607)。通信データの通信内容が改ざんされていなかったと判断する(ステップ1610)。通信データの通信内容が改ざんされていると判断する(ステップ1611)。

【0078】検閲プログラム1101の動作手順を図17の流れ図で説明する。

【0079】変数Iに「1」をセットする(ステップ1701)。外部記憶装置513にある検閲ワードテーブル1102のI番目のワードデータを取り出す。ワードが取り出せれば、ステップ1703へ進む。取り出せなければ、終了する(ステップ1702)。

【0080】ステップ1702で取り出したワードデータをキーに与えられた通信内容を検索する。検索がマッチすればステップ1704へ、通信内容を最後まで検索したらステップ1705へ進む(ステップ1703)。通信内容の検索がマッチしたワードの全文字をを検閲文字に置き換える。そして、ステップ1703へ戻る(ステップ1704)。

【0081】次に、変数Iの値を「1」増やし、ステップ1802に戻る(ステップ1705)。

【0082】

【発明の効果】本発明により、以下の示す2つの効果が得られる。

【0083】1) 検閲により通信内容の変更があった場合でも通信内容の最終的な受信者がデータの完全性をチェックできる。

【0084】2) 通信内容の検閲の履歴を送信者が全て記録できるので、検閲者もしくは、検閲プロセスが複数いた時にどの検閲者もしくは、検閲プロセスがどの部分を削除したか判別することができる。

【図面の簡単な説明】

【図1】デジタル署名による認証方法に必要な要素を示す構成図である。

【図2】デジタル署名による認証方法の処理手順を示す流れ図である。

【図3】図8の通信内容に対するデジタル署名を示した図である。

【図4】本発明の実施形態の基本構成を示すシステム構成図である。

【図5】送信者のワークステーションの基本構成を示す

システム構成図である。

【図6】デジタル署名用の設定パラメータを格納するテーブルの構成図である。

【図7】履歴情報を格納するテーブルの構成図である。

【図8】通信内容の例を示した図である。

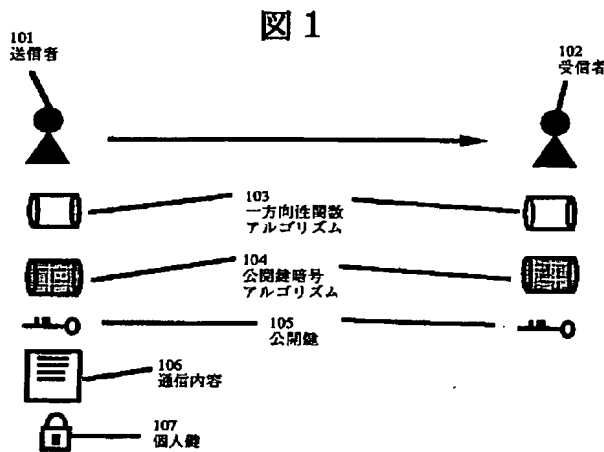
【図9】ワークステーション間で通信される情報のデータ構造を示した構成図である。

【図10】検閲者のワークステーションの基本構成図を示すシステム構成図である。

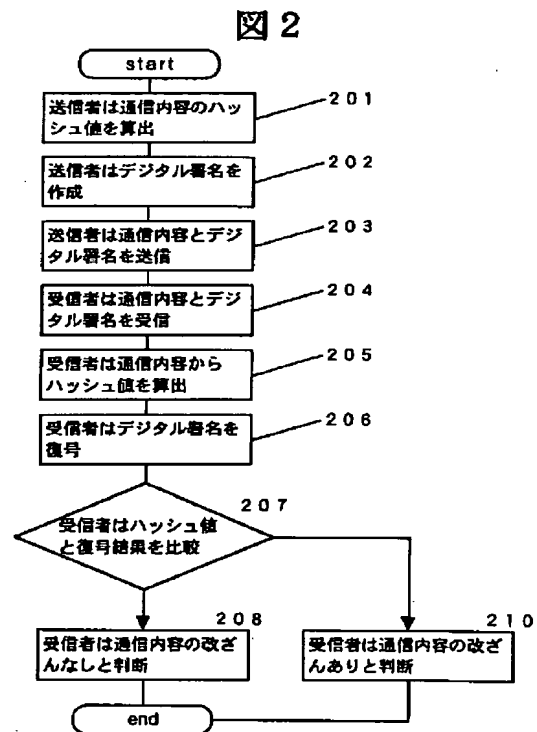
【図11】検閲ワードを格納するテーブルの構成図である。 10

【図12】受信者のワークステーションの基本構成を示すシステム構成図である。 \*

【図1】



【図2】



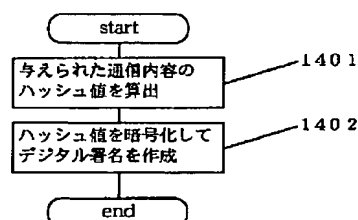
【図3】

図3

P7xWc9MrfzJVvmhLYEjkdP+6+UZ8Vh38eREbMD+c8NEZ77VUmMhobDGssZ8Yel  
p78XLmPUR5pT5HX2paA6Jw==

【図14】

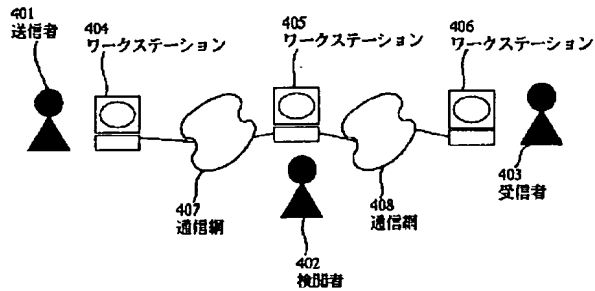
図14





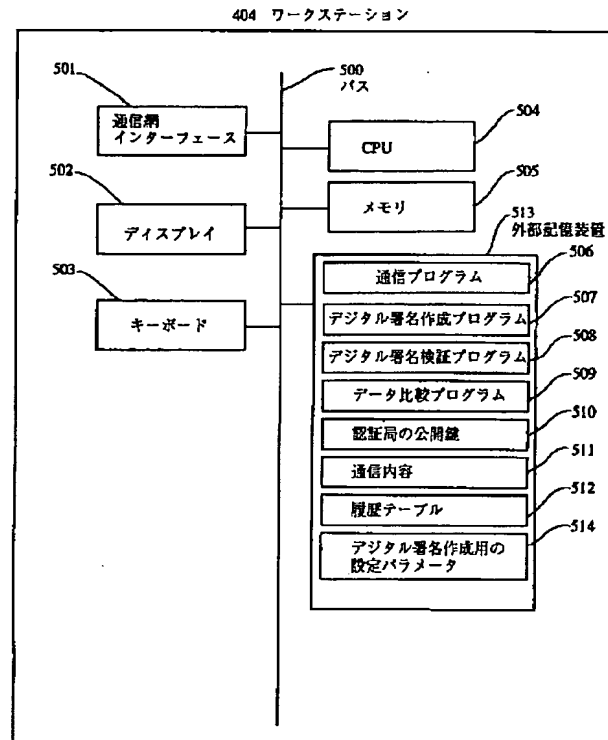
【図4】

図4



【図5】

図5



【図6】

図6

| 600<br>一方性関数<br>アルゴリズム<br>識別子 | 601<br>公開鍵暗号<br>アルゴリズム<br>識別子 | 602<br>個人鍵 | 603<br>公開鍵 | 604<br>デジタル署名 |
|-------------------------------|-------------------------------|------------|------------|---------------|
| MD5                           | RSA512                        | 2e9f...    | 13a7...    | ehj0io...     |
| MD5                           | RSA1024                       | 5a8d...    | be7a...    | uhld3o...     |
| ⋮                             | ⋮                             | ⋮          | ⋮          | ⋮             |

【図7】

図7

| 701<br>検閲前の<br>通信内容 | 702<br>デジタル<br>署名 | 703<br>一方性関数<br>アルゴリズム<br>識別子 | 704<br>公開鍵暗号<br>アルゴリズム<br>識別子 | 705<br>検閲後の<br>通信内容 | 706<br>デジタル<br>署名 | 707<br>署名者 | 708<br>公開鍵 |
|---------------------|-------------------|-------------------------------|-------------------------------|---------------------|-------------------|------------|------------|
| 13a7...             | 2e9f...           | MD5                           | RSA512                        | uhld3o...           | 13a7...           | take       | ehj0io...  |
| be7a...             | 5a8d...           | MD5                           | RSA1024                       | 5a8d...             | be7a...           | basi       | uhld3o...  |
| ⋮                   | ⋮                 | ⋮                             | ⋮                             | ⋮                   | ⋮                 | ⋮          | ⋮          |

【図8】

図 8

```

bonsal% hping
PING hskgw.hitachi-sk.co.jp: 56 data bytes
64 bytes from hskgw.hitachi-sk.co.jp (133.107.1.2): icmp_seq=0. time=685. ms
64 bytes from hskgw.hitachi-sk.co.jp (133.107.1.2): icmp_seq=1. time=690. ms
64 bytes from hskgw.hitachi-sk.co.jp (133.107.1.2): icmp_seq=2. time=480. ms
64 bytes from hskgw.hitachi-sk.co.jp (133.107.1.2): icmp_seq=3. time=699. ms
64 bytes from hskgw.hitachi-sk.co.jp (133.107.1.2): icmp_seq=4. time=689. ms
64 bytes from hskgw.hitachi-sk.co.jp (133.107.1.2): icmp_seq=5. time=900. ms
64 bytes from hskgw.hitachi-sk.co.jp (133.107.1.2): icmp_seq=6. time=648. ms
64 bytes from hskgw.hitachi-sk.co.jp (133.107.1.2): icmp_seq=7. time=973. ms
64 bytes from hskgw.hitachi-sk.co.jp (133.107.1.2): icmp_seq=8. time=917. ms
64 bytes from hskgw.hitachi-sk.co.jp (133.107.1.2): icmp_seq=9. time=614. ms

--- 2.1.107.133.in-addr.arpa PING Statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 480/709/973
△山〇男

```

【図9】

図 9

901 通信データ

902 通信内容

912 署名者パラメータ部

903 デジタル署名 = MF8xCzAJBgNVBAYTAkdCMStwIAYDVQQK

904 KEsIVbml2ZXJzaXRlbnVbGxIZ2UgTG9uZuMRkwFwYDVQQQ1

905 署名者名 = へのへのへ

906 公開鍵 = P7xWc9MrFZJVmHLVvEjrdP+6+UZ8VUmMhob

907 D6QQLExBDb21

909 公開鍵のデジタル署名 = DVL8DwdXRiciBTYlbnMlMRwD

910 TV09SPxcMFjmlVjIP+6+UZ8Vh38eREbMldP+6+UZ8Vh38

913 署名者パラメータ部

907 デジタル署名 = MF8xCzAJBgNVBAYTAkdCMl2ZXJzaXRl

908 BnVbGxIZ2UgTG9uZG9uMRkwFwYDVQQLEsBDb21

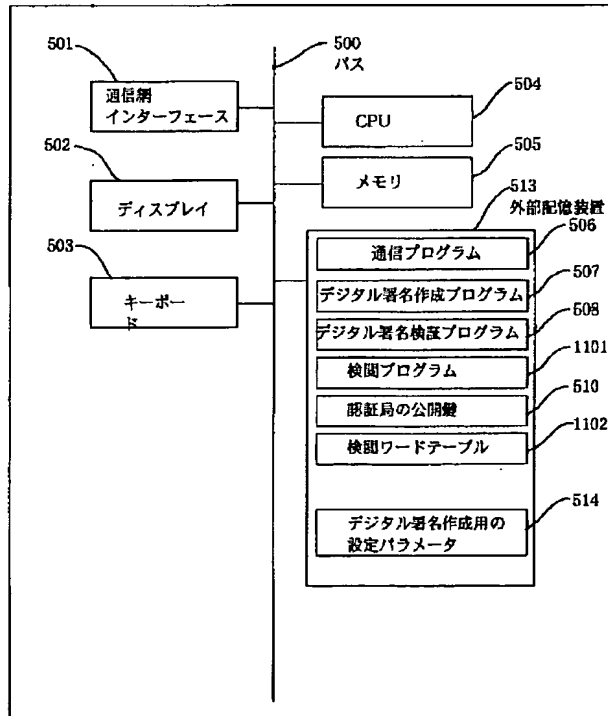
署名者名 = へのへのへ

...

【図10】

図 10

405 ワークステーション



【図11】

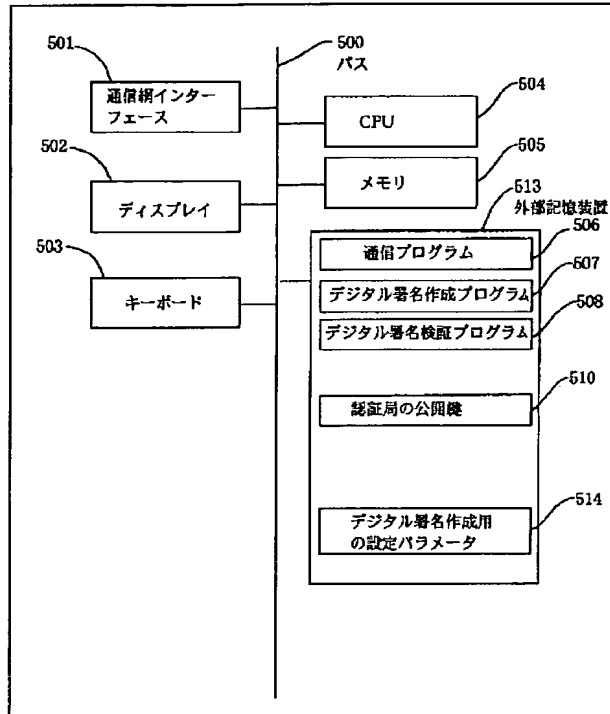
図 11

| #   | ワードデータ      |
|-----|-------------|
| 1   | 携帯端末課       |
| 2   | Windows MT課 |
| ... | ...         |

【図12】

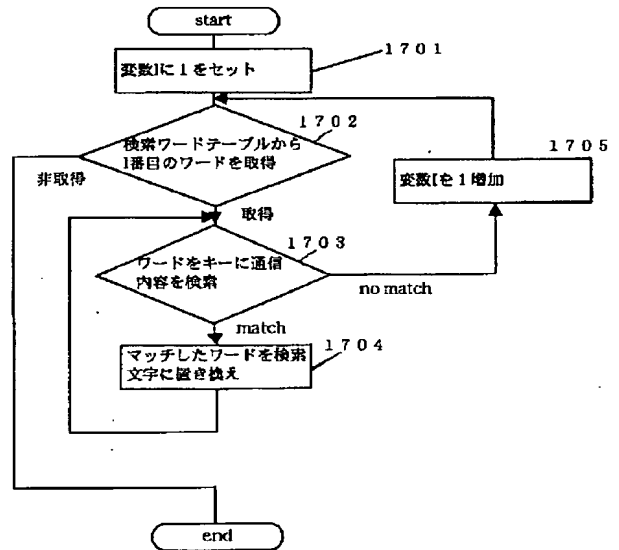
図12

406 ワークステーション



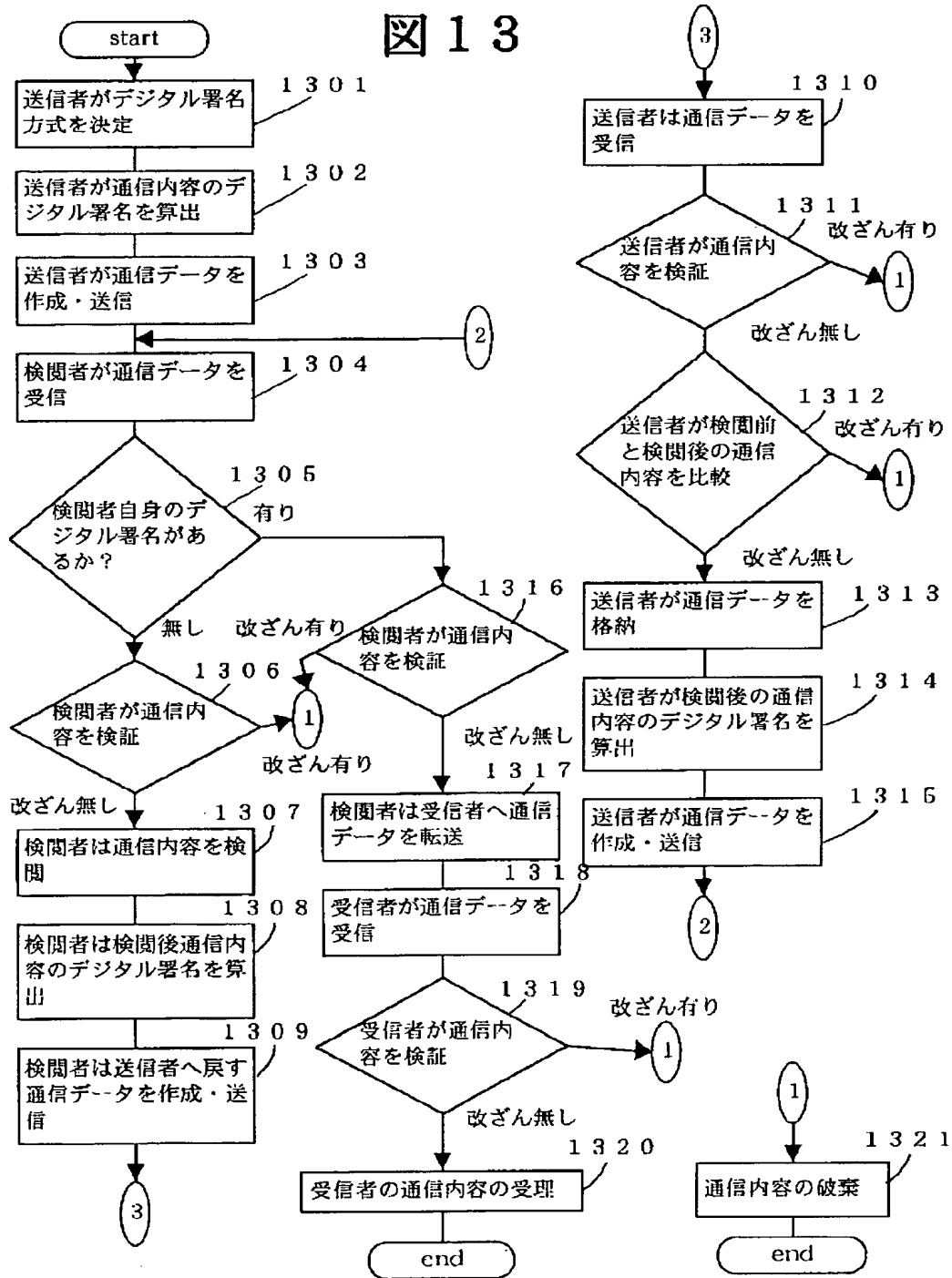
【図17】

図17



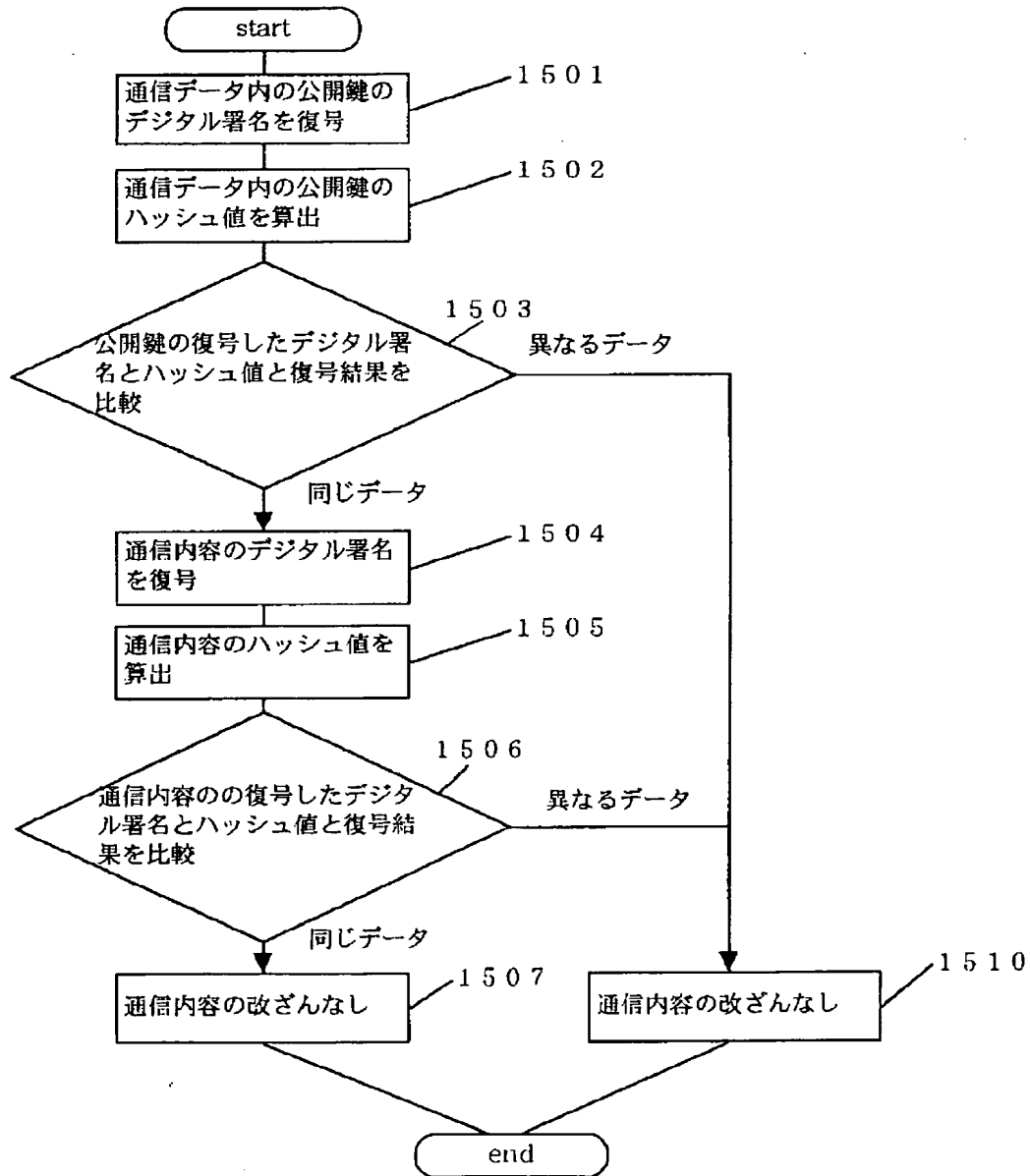
【図13】

図 13



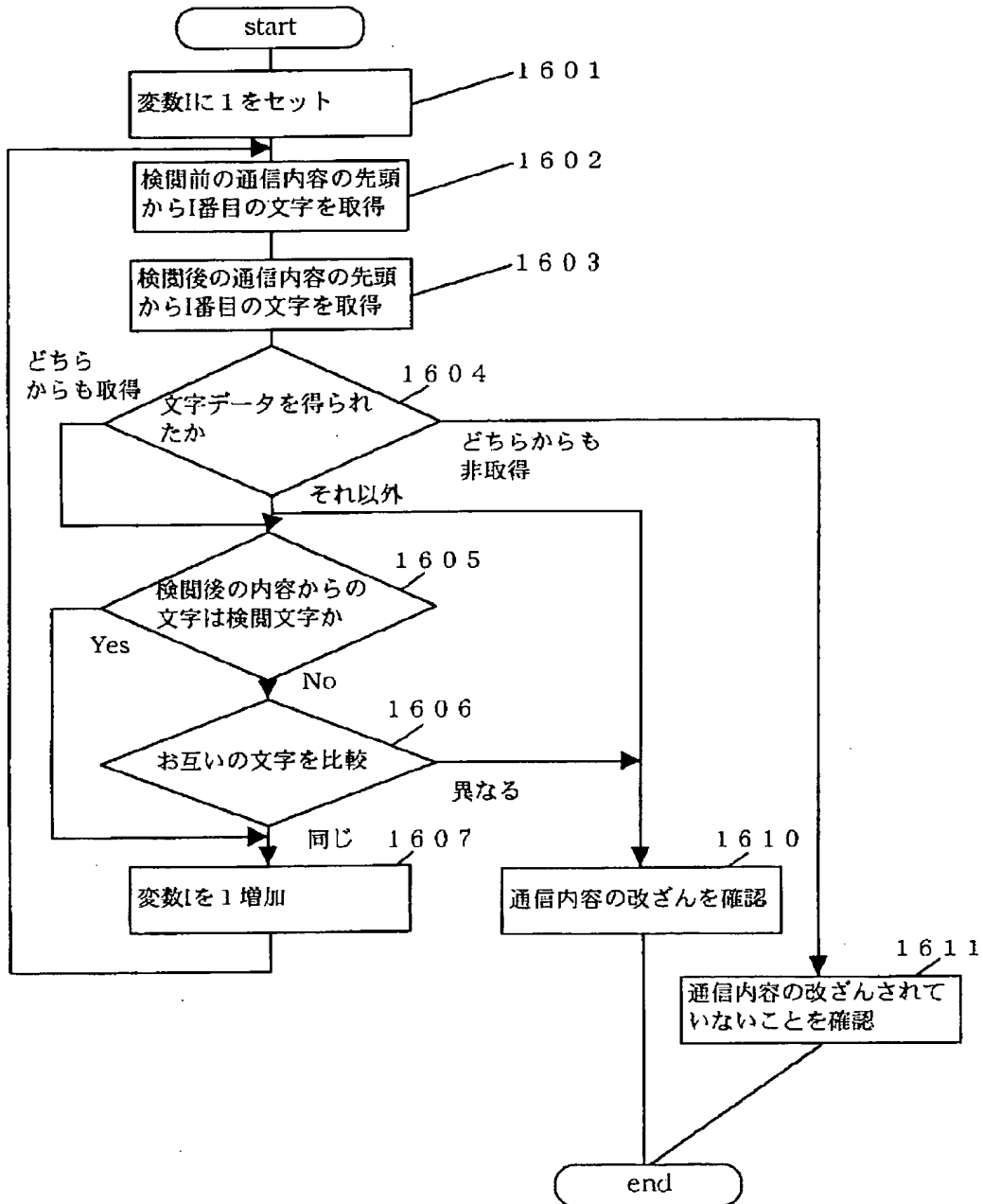
【図15】

図 15



【図16】

## 図 16



【公報種別】特許法第17条の2の規定による補正の掲載  
 【部門区分】第6部門第2区分  
 【発行日】平成14年1月23日(2002.1.23)

【公開番号】特開平10-105058  
 【公開日】平成10年4月24日(1998.4.24)  
 【年通号数】公開特許公報10-1051  
 【出願番号】特願平8-254057  
 【国際特許分類第7版】  
 G09C 1/00 640

【F1】  
 G09C 1/00 640 Z  
 640 D  
 640 E

【手続補正書】  
 【提出日】平成13年6月12日(2001.6.12)  
 【手続補正1】  
 【補正対象書類名】明細書  
 【補正対象項目名】発明の名称  
 【補正方法】変更  
 【補正内容】  
 【発明の名称】データ保証システムおよびデータ保証方法

【手続補正2】  
 【補正対象書類名】明細書  
 【補正対象項目名】特許請求の範囲  
 【補正方法】変更  
 【補正内容】  
 【特許請求の範囲】

【請求項1】 通信網によって相互に接続された複数の端末からなり、送信者と受信者との間で通信される通信データが通信経路間の検閲端末により検閲処理されるデータ保証システムであって、  
前記検閲端末は、送信元の端末から送信された通信データを検閲する手段と、  
検閲後の通信データと検閲前の通信データとを、前記検閲端末のデジタル署名とともに送信元の端末に返送する手段とを有し、  
前記送信元の端末は、前記検閲後の通信データが返送されてきた場合に、前記検閲前の通信データと、前記検閲後の通信データとを比較して通信データの改ざんがないかを検証し、改ざんがない場合に、前記検閲後の通信データに対してデジタル署名を行う手段と、  
前記検閲端末を介して、前記検閲後の通信データを受信先の端末に送信する手段とを有することを特徴とするデータ保証システム。

【請求項2】 通信網によって相互に接続された複数の端末からなり、送信者と受信者との間で通信される通信データが通信経路間の検閲端末により検閲処理されるデータ保証システムにおけるデータ保証方法であって、  
前記検閲端末において、送信元の端末から送信された通信データを検閲し、検閲後の通信データと検閲前の通信データとを、前記検閲端末のデジタル署名とともに送信元の端末に返送し、  
前記送信元の端末において、前記検閲後の通信データが返送されてきた場合に、前記検閲前の通信データと、前記検閲後の通信データとを比較して通信データの改ざんがないかを検証し、改ざんがない場合に、前記検閲後の通信データに対してデジタル署名を行い、前記検閲端末を介して、前記検閲後の通信データを受信先の端末に送信することを特徴とするデータ保証方法。

【手続補正3】  
 【補正対象書類名】明細書  
 【補正対象項目名】0011  
 【補正方法】変更  
 【補正内容】

【0011】次に、受信者102はステップ203で送信された通信内容106とデジタル署名を受信する(ステップ204)。

【手続補正4】  
 【補正対象書類名】明細書  
 【補正対象項目名】0021  
 【補正方法】変更  
 【補正内容】  
 【0021】

【課題を解決するための手段】この課題を解決するため、本システムでは、検閲者もしくは、検閲プロセスが削除・変更した通信内容を送信者に戻して新たに通信内

容の完全性を保証するデジタル署名を計算することを提案する。この時、送信者が常に返送される変更・修正された通信内容を監視する必要は無く、自動的にデジタル署名を行い、受信者に再送信される。即ち、本発明は、通信網によって相互に接続された複数の端末からなり、送信者と受信者との間で通信される通信データが通信経路間の検閲端末により検閲処理されるデータ保証システムにおいて、前記検閲端末において、送信元の端末から送信された通信データを検閲し、検閲後の通信データと検閲前の通信データとを、前記検閲端末のデジタル署名とともに送信元の端末に返送し、前記送信元の端末において、前記検閲後の通信データが返送されてきた場合に、前記検閲前の通信データと、前記検閲後の通信データとを比較して通信データの改ざんがないかを検証し、改ざんがない場合に、前記検閲後の通信データに対してデジタル署名を行い、前記検閲端末を介して、前記検閲後の通信データを受信先の端末に送信することを特徴とする。

【手続補正 5】

【補正対象書類名】明細書

【補正対象項目名】0024

【補正方法】変更

【補正内容】

【0024】ワークステーション404とワークステーション405は通信網407を介して相互に通信を行うことができ、ワークステーション405とワークステーション406は通信網408を介して相互に通信を行うことができる。そして、ワークステーション404とワークステーション406は、通信網407とワークステーション405と通信網408を介して通信を行うことができる。送信者401や検閲者402、受信者403は、ユーザ、あるいは、プログラムを示している。

【手続補正 6】

【補正対象書類名】明細書

【補正対象項目名】0037

【補正方法】変更

【補正内容】

【0037】図11は検閲ワードテーブル1102の例を示す図である。検閲ワードテーブル1102は検閲者のポリシーが反映されており、例えば、外部に開示したくない組織内のサブ組織名や製品のコードネームや露骨でひくい表現や相手を侮辱する表現などが格納されている。

【手続補正 7】

【補正対象書類名】明細書

【補正対象項目名】0047

【補正方法】変更

【補正内容】

【0047】次に、検閲者402はワークステーション

405の外部記憶装置513にある検閲プログラム1101に、ステップ1306で改ざんされていないことを確認された通信内容を与えて、ワークステーション405のメモリ505上で実行させて、検閲後の通信内容を得る。ここで、通信内容の検閲は、検閲プログラム1101で行わないで、人間である検閲者が手動で行う場合も想定している（ステップ1307）。

【手続補正 8】

【補正対象書類名】明細書

【補正対象項目名】0051

【補正方法】変更

【補正内容】

【0051】次に、送信者401はワークステーション404の外部記憶装置513にあるデジタル署名検証プログラム508に、ステップ1310で受信した2つの通信データをそれぞれ個別に与えて、ワークステーション404のメモリ505上で実行させ、通信データ内の通信内容が改ざんされていないか確認する。どちらか一方の通信内容が改ざんされていればステップ1321へ進む。どちらも改ざんされていなければステップ1312へ進む（ステップ1311）。

【手続補正 9】

【補正対象書類名】明細書

【補正対象項目名】0053

【補正方法】変更

【補正内容】

【0053】次に、送信者401はステップ1310で受信した2つの通信データのコピーを外部記憶装置513の履歴テーブルに格納する（ステップ1313）。

【手続補正 10】

【補正対象書類名】明細書

【補正対象項目名】0063

【補正方法】変更

【補正内容】

【0063】改ざんがあった場合、送信者401、検閲者402、受信者403、いずれの場合も通信データを全て消去する（ステップ1321）。

【手続補正 11】

【補正対象書類名】明細書

【補正対象項目名】0080

【補正方法】変更

【補正内容】

【0080】ステップ1702で取り出したワードデータをキーに与えられた通信内容を検索する。検索がマッチすればステップ1704へ、通信内容を最後まで検索したらステップ1705へ進む（ステップ1703）。通信内容の検索がマッチしたワードの全文字を検閲文字に置き換える。そして、ステップ1703へ戻る（ステップ1704）。